Major threats this month for Windows:

Microsoft patches critical flaws in Windows, IE, Office. Attackers could exploit any of the flaws to take over unpatched machines, and exploit code is already circulating.

Where you can read more on this story:

Where to get the Latest Patches:
Windows/Office update site at

Remember: Hackers already know how to utilize these holes within your programs to get into the computer. See the below link for examples on how to patch your computer.


Other Patch Sites:

Several Patch Sites for various applications and Windows Updates:
http://www.softwarepatch.com
https://patches.mont.disa.mil/index.jsp (.mil address only)
https://ceds.ssg.gunter.af.mil/enosc/index.asp (.mil address only)

Patch Sites for various applications and updates for Macintosh OS X

Phishing Alerts - What To Avoid This Month (currently approximately 161 alerts) information also available at
http://www.millersmiles.co.uk/archives/current

I. Top Rated Phishing threat emails from people trying to get you to divulge private details. These are often trying to steal your identity (and your money)

I.1 LaSalle Bank-'IMPORTANT: Account Verification'
I.2 Sky - 'Sky Informs You!'
I.3 NCUA - '*** WARNING: Security Issues ***'

II. Virus and Hoax Alerts
II.1 Troj/Torpig-A (Trojan)
II.2 Troj/Fishnat-A (Phishing Trojan)
II.3 Troj/Bancsde-E (Phishing Trojan)

III. General Phishing/Email Information
III.2 Identity Theft
IV. Online Data Gets Personal: Cell Phone Records for Sale

V. Hackers Skip Windows to Embed New Infections

VI. Worm Spreads Through AOL Instant Messenger

VII. Hackers to feast on data via Bluetooth 'war nibbling'

VIII. Breaches of customers' data trigger lawsuits

IX. Arrests/Convictions
   IX.1 Teen Worm Writer Fined 1,000 Euros
   IX.2 Spammer Could Face Three-Year Prison Sentence
   IX.3 Two UK Men Sentenced in Phishing Scheme
   IX.4 Alleged Spammer First to be Tried Under Australia's Spam Law

X. US-CERT Warns of Latest Trojan Horse Attacks

XI. It is Quiz Time

More Details About Things To Avoid

I. Email from people trying to steal your identity (and your money)
   I.1 LaSalle Bank-'IMPORTANT - Account Verification'
      The Bait: Informing you that the bank has a new security
               system and ensuring that security is being met.
      The Goal: To get you to enter credit card information, ATM PIN
               number, and SSN.

      Where you can see how it actually appears:
      http://www.antiphishing.org/phishing_archive/06-22-05_LaSalle/06-22-05_LaSalle.html

   I.2 Sky - 'Sky Informs You!'
      The Bait: Email stating that your account may have had
               unauthorized third party activity.
      The Goal: To capture your credit card information, and ATM PIN
               number, social security #, etc.

      Where you can see how it actually appears:
      http://www.antiphishing.org/phishing_archive/06-28-05_Sky/06-28-05_Sky.html

   I.3 NCUA - '*** WARNING: Security Issues ***'
      The Bait: Email that is asking you to verify your account
               Information for security reasons.
      The Goal: To capture your credit card information, ATM PIN number.
II. Virus and Hoax Alerts:

II.1 Troj/Torpig-A (Trojan)

Delivery Method: This Trojan downloads and executes additional files from a remote site. Configuration files may also be downloaded that define further behaviors.

Effects of Infection: This Trojan will turn off your anti-virus applications, allows others to access the computer, modifies data on the computer, steals information, and is dropped by malware.

Where you can read more on this: http://www.sophos.com/virusinfo/analyses/trojtorpiga.html

II.2 Troj/Fishnat-A (Phishing Trojan)

Delivery Method: The Trojan appears to be a login page for a prominent banking site. The login details are sent to a remote user via email.

Effects of Infection: This particular Phishing Trojan will try to steal your personal information.

Where you can read more on this: http://www.sophos.com/virusinfo/analyses/trojfishnata.html

II.3 Troj/Bancsde-E (Phishing Trojan)

Delivery Method: It can be delivered through a web site.

Effects of Infection: Allows others to access the computer, steals information, reduces system security, records keystrokes, installs itself in the Registry and dropped by malware.

Where you can read more on this: http://www.sophos.com/virusinfo/analyses/trojbancsdee.html

III. Phishing Information:

III.1 Email schemes, called "Phishing" or "carding," are an attempt to trick consumers into disclosing personal or financial information.

Where you can read more on this story: http://www.atg.wa.gov/consumer/idprivacy/phishing.shtml

IV. Online Data Gets Personal: Cell Phone Records for Sale

They're not just after your credit card or Social Security numbers. Fuelled by the ease of online commerce, they are on the
trail of other personal information as well.

Where you can read more on this story:
http://www.washingtonpost.com/wp-dyn/content/article/2005/07/07/AR2005070701862_pf.html

**********************
V. Hackers Skip Windows to Embed New Infections

Flaws in software that can be exploited by hackers are on the rise, said the report by the SANS Institute of Bethesda, a cyber-security research and education center.

Where you can read more on this story:

**********************
VI. Worm Spreads Through AOL Instant Messenger

The worm spread in instant messages with the text: "LOL LOOK AT HIM" and included a Web link to a file called "picture.pif."

Where you can read more on this story: http://news.zdnet.com/2100-1009_22-5748646.html

**********************
VII. Hackers to feast on data via Bluetooth 'war nibbling'

Bluetooth is beginning to appear in more and more devices, from PDAs and laptops to cell phones. Unlike 802.11-based wireless LANs, which have a range of as much as 100 yards or more, these have short ranges of only 30 feet but can be easily intercepted.

Where you can read more on this story:
http://searchmobilecomputing.techtarget.com/gna/0,289202,sid40_gci932089,00.html

**********************
VIII. Breaches of customers' data trigger lawsuits

Some banks last month notified many consumers that computer hackers had filched their credit card and debit card information.

Where you can read more on this story: http://www.postgazette.com/pg/05202/541454.stm

**********************
IX. Arrests and Convictions

IX.1 While the English-language press reported that 19-year-old Sven Jaschan confessed on Tuesday that he was the creator of the "Sasser" worm, the German Press Agency rushed ahead with some fresh news on this.
IX.2 A Florida man could face a prison sentence of up to three years for sending unsolicited email messages. Peter Moshou said he would plead guilty to one count of violating the CAN-SPAM Act.

IX.3 Two men have been sentenced to a total of 10 years in prison for their roles in a wide range of online fraud activities.

IX.4 The Australian government has joined the legal counterattack against spam by taking an alleged spammer to court.

X. US-CERT Warns of Latest Trojan Horse Attacks

US-CERT (the US Computer Emergency Readiness Team), issued an alert today warning of heightened Trojan virus attacks against companies and individuals. While there were numerous reports of slowdowns at various Web sites, the cause has largely been attributed to increased Web use following the Live multi-venue concert event and the terrorist bombings in London.

Ken Silva, chief security officer at Verisign, referred to the CERT alert and said the slowness among some corporate Web sites on Monday is due to targeted Trojan horse attacks.

For more details visit:
http://www.esecurityplanet.com/alerts/article.php/3519236

XI. It is Quiz Time

Here are two great quizzes that we have found on the net that have valuable information for you, your coworkers and family to help them with Phishing and staying safe online.

http://searchsecurity.techtarget.com/general/0,295582,sid14_gc1101641,00.html
http://searchsecurity.techtarget.com/generic/0,295582,sid14_gc11090227,00.html

Copyright 2005, The SANS Institute. Permission is hereby granted for any person to redistribute this in whole or in part to any other
persons as long as the distribution is not being made as part of any commercial service or as part of a promotion or marketing effort for any commercial service or product.